AFFIDAVIT OF TASK FORCE OFFICER BRIAN BISCEGLIA

I, Brian Bisceglia, being duly sworn, hereby depose and say:

1. I am a Task Force Officer currently assigned to the Federal Bureau of Investigation ("FBI"), Boston Division Child Exploitation Task Force. I have been employed by the City of Worcester as a police officer for approximately 14 years and have been assigned to the Detective Bureau for approximately five years. I was also employed by the Town of Holden as a part-time police officer for approximately five years. I have Bachelor of Science degree from Wentworth Institute of Technology and attended Northeastern University. I was also previously employed for more than ten years as a design engineer for 3Com, Ciena, Avaya, and other communication and/or computer companies. I am listed as inventor/co-inventor on three US patents (patent numbers: 8098681, 6275498, and 6066001). During my career, I have investigated misdemeanor and felony crimes to include violent crimes, homicides, and child exploitation cases. I have obtained and executed multiple search warrants during my career. Additionally, I am member of the Internet Crimes Against Children ("ICAC") task force maintained by the Department of Justice.

2. I submit this affidavit in support of an application for a warrant authorizing the search of 16 Eustis Street, Worcester, Massachusetts (hereinafter, the "SUBJECT PREMISES"), as further described in Attachment A. As detailed below, probable cause exists to believe that contraband and/or the evidence, fruits, or instrumentalities of a crime, namely the possession of child pornography in violation of 18 U.S.C § 2252A(a)(5)(B), are presently located at the SUBJECT PREMISES. Accordingly, I request authority to search the entire SUBJECT

PREMISES, including any computer and computer media located therein, and to seize those items specified in Attachment B, attached hereto.

3. The evidence described in Attachment B includes evidence maintained in electronic format on any computer and computer media within the SUBJECT PREMISES. The methods by which the electronic information will be searched are more fully set forth in the "Computer Evidence" section of this affidavit.

4. The information set forth in this affidavit is based on an investigation conducted by law enforcement agents, including myself. This affidavit does not contain every fact known to me with respect to this investigation. Rather, it contains those facts that I believe necessary to establish probable cause for issuance of the requested warrant to search the SUBJECT PREMISES.

RELEVANT STATUTES

5. Title 18, United States Code, Section 2252A(a)(5)(B), makes it illegal for any person to knowingly possess child pornography, in or affecting interstate or foreign commerce. Section 2252A(a)(5)(B) specifically refers to a computer as one means by which a visual depiction may travel in and/or otherwise affect interstate commerce.

6. "Child pornography" is defined in Title 18, United States Code, Section 2256(8) as "any visual depiction … of sexually explicit conduct, where – (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual

depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct."

THE SUBJECT PREMISES

7. The SUBJECT PREMISES is located at 16 Eustis Street, in Worcester, Massachusetts. The SUBJECT PREMISES is a tan ranch-style home with brown shutters, a brown front door, and an attached one-car garage that is located under the main floor. The garage has a large, bowed, picture window located above it. The number "16" is clearly displayed on the siding located to the left of the front door. Public records identify the residence as a three bedroom, single family residence. A photograph of the SUBJECT PREMISES is included in Attachment A.

INSTANT INVESTIGATION

8. The National Center for Missing and Exploited Children ("NCMEC") was established in 1984 as a private, nonprofit 501(c)(3) organization to provide services nationwide for families and professionals in the prevention of abducted, endangered, and sexually exploited children. NCMEC's mission is to help prevent child abduction and sexual exploitation, help find missing children, and assist victims of child abduction and sexual exploitation, their families, and the professionals who serve them. Pursuant to its mission and its congressional mandates (*see* 42 U.S.C. § 5771 *et seq.;* 42 U.S.C. § 11606; 22 C.F.R. § 94.6), NCMEC serves as a clearinghouse of information about missing and exploited children and operates a "CyberTipline" (aka "Cybertip") that the public may use to report Internet-related child sexual exploitation.

9. The CyberTipline is a reporting mechanism for incidents of child sexual exploitation, including child pornography, online enticement of children for sex acts, molestation

of children outside the family, sex tourism of children, child victims of prostitution, and unsolicited obscene material sent to a child. Reports may be made 24-hours a day, 7 days a week either online or by calling a toll free number.

10. In 1996, Congress established the Exploited Child Unit ("ECU") within NCMEC. In addition to handling reports received via the CyberTipline, the ECU serves as a technical and informational resource for law enforcement. As such, the ECU is highly experienced in identifying child pornography. Furthermore, the ECU maintains a database of images that depict identified victims of child pornography.

11. On or about October 13, 2015, NCMEC forwarded CyberTipline Report 6695869 ("Report 6695869") to Massachusetts State Police. Report 6695869 contained information regarding suspected child pornography that Photobucket.com ("Photobucket"), an electronic service provider, provided to NCMEC on September 30, 2015. Photobucket was listed in the report as located at 2399 Blake Street #160, Denver, Colorado 80205.

12. According to the information contained in Report 6695869, a user of Tinypic.com,[1] an internet site maintained by Photobucket, uploaded a video to the Tinypic.com website that Photobucket personnel believed constituted child pornography. Report 6695869 indicated that the video, identified by filename **iqg9z8.flv**, was uploaded from IP address 75.143.45.188 on September 11, 2015 at 01:59:25 p.m. MDT. NCMEC transmitted video file **iqg9z8.flv**, along with the Report 6695869, to Massachusetts State Police.

13. Report 6695869 also indicated that Charter Communications ("Charter") was the

[1] As discussed in further detail below, Tinypic.com is a photo and video sharing service, owned and operated by Photobucket.com, that allows users to upload, link and share, images and videos on the Internet.

internet service provider responsible for hosting IP address 75.143.45.188 on September 11, 2015.

14. On October 15, 2015, Trooper James Dowling, assigned to the ICAC Task Force, served an administrative subpoena upon Charter. In response to the subpoena, Charter provided records that identified Nicole Griffin, 16 Eustis Street, Worcester, Massachusetts 01606, as the subscriber to whom IP address 75.143.45.188 was assigned from September 4, 2015 at 15:37:24 GMT to October 19, 2015 at 19:26:43 GMT.

15. I received a copy of Report 6695869 from Trooper Dowling on or about Thursday, November 16, 2015 and reviewed video file **iqg9z8.flv** on or about that same date. Based upon my training and experience, the video constitutes child pornography. Specifically, video file **iqg9z8.flv** depicts a prepubescent, minor male (whose face can be seen) performing oral sex on an adult male (whose face cannot be seen). The minor male is kneeling in front of the adult male who ejaculates into the minor male's hands at the end of the video.

16. On November 23, 2015, a public records database search for 16 Eustis Street Worcester, Massachusetts identified several possible residents. The most recent residents were identified as follows:

- Nicole Griffin, born 1976;
- Tyler Griffin, born 1994, and
- William Ferrante, born 1988.

17. On January 7, 2016, a query of the Massachusetts Registry of Motor Vehicles ("RMV") database returned the following information regarding 16 Eustis Street, Worcester, Massachusetts:

- An active driver's license for Nicole Griffin, born 1976;
- A Massachusetts identification card for Tyler Griffin, born 1994;
- An expired driver's license for William Butler, born 1971; and,
- An expired driver's license for Bonnie Butler, born 1975.

18. A query of the RMV database for Ferrante identified a suspended driver's license that was issued on February 5, 2013, with a mailing address of 21 Mill Street, Webster, Massachusetts.

19. A parcel search of the Worcester public records website for 16 Eustis Street within the City of Worcester identified the residence as a single family home currently owned by Nicole Griffin.[2] A www.masslandrecords.com query on January 7, 2016, identified Griffin as the owner since August 5, 2009.[3]

20. Investigators ran criminal history queries of the Massachusetts Board of Probation ("BOP") database for Nicole Griffin, Tyler Griffin and William Ferrante. The query for Ferrante yielded the following results:[4]

(a) On April 4, 2013, Ferrante admitted sufficient facts in Dudley District Court on the charge of Impersonation of a Police Officer, and the court continued the matter without a finding until April 1, 2014. On July 16, 2013, the district court found Ferrante in violation of his probation and sentenced him to one year committed in the House of Corrections;

(b) On July 16, 2013, Ferrante was convicted in Dudley District Court for Enticement of a Child under 16. The Court sentenced Ferrante to 2½ years in the House of Corrections; and

---

[2] The City of Worcester public records website is located at http://www.worcesterma.gov/e-services/search-public-records/property-values

[3] The grantors of the property are identified as Leo Butler and Margaret Butler.

[4] Nicole Griffin was charged in Massachusetts as a juvenile with breaking and entering in the daytime (1993). That charge was continued without a finding by the court. She was also charged in Rhode Island for disorderly conduct (2012). The disposition of that charge is unknown. Tyler Griffin was previously charged in Massachusetts with misdemeanor larceny (2013) and vandalism (2014). Both of those charges were continued without a finding.

(c) On November 25, 2013, Ferrante was convicted in Dudley District Court for Possession of Child Pornography. The court sentenced Ferrante to probation until November 28, 2017.

21. Ferrante is registered as a level two Sex Offender. Ferrante's BOP identified the Webster Police Department as the arresting agency for the above-detailed offenses.

22. On January 4, 2016, Worcester Superior Court Probation Officer Maura Tatro confirmed that Ferrante is currently on probation out of the Worcester District Court. Ferrante has reported his address as 16 Eustis Street, Worcester, Massachusetts since July 1, 2015. He most recently confirmed that address to probation on December 30, 2015.

23. I spoke again with Maura Tatro on Wednesday, January 13, 2016. Tatro informed me that probation records indicate that Probation Officer Hanh Nguyen conducted a scheduled home visit with Ferrante at 16 Eustis Street in Worcester on Monday, January 11, 2016. According to those records, Ferrante provided information to Nyugen at that time regarding his employment status.

24. Webster Police provided investigators with the reports that correspond to the three convictions described in paragraph 20. The following is a summary of the three incidents as reported by Webster Police:

(a) On March 11, 2013, a female driver traveling south on Route 395 in Oxford noticed a vehicle behind her with a blue light on. The female pulled over, allowed the vehicle to pass, and then resumed travel on Rte. 395. The vehicle slowed down, got back behind her vehicle and again turned on the blue light. The female called her boyfriend, who directed her to drive directly to his residence. The vehicle followed and stopped behind her after she pulled into her boyfriend's driveway, where her boyfriend was waiting. The driver of the vehicle, later identified as William Ferrante, got out of his vehicle and demanded the female's driver's license. When the boyfriend asked which police department Ferrante was with, Ferrante stated that he was an off-duty military police officer and that he

just wanted to warn the female driver that she was speeding. Ferrante then left the area. Webster Police arrested and interviewed Ferrante, who admitted to using a blue light to stop the vehicle. Ferrante told Webster Police that he had been trying to get into Colorado Tech's information technology program so he could get into the FBI. He further stated that he wanted to be a police officer or firefighter from the age of six and that type of work was in his blood. He also stated that he was a juvenile sex offender in Rhode Island and that that record was sealed.[5]

(b) On May 5, 2013, a parent reported to Webster Police that "Alex Salazarri" had contacted their 10 year old son and requested various sexual acts. Webster Police identified "Alex Salazarri" as William Ferrante. Their investigation showed that William Ferrante met the boy at a skate park in Webster and brought the boy to the campsite located in the woods of Webster where Ferrante lived. While at the campsite, Ferrante asked the child if he could perform oral sex on the boy or if Ferrante could masturbate in front of the child. The child refused and left without engaging in sex with Ferrante. Ferrante told the Webster Police that he would hang around the skate park to mentor children and help them with their homework, and that he bought XBox time credits as an incentive for children who did well in school. He told Webster Police that he had completed a sex offender program in Rhode Island and that he had a problem with exhibitionism.

(c) On or about September 8, 2013, Webster Police conducted follow-up investigation of the May 5, 2013 incident. During that arrest, Webster Police seized Ferrante's cell phone. Webster Police forensically examined the phone and found over 100 images of child pornography. Webster Police estimated the ages of children involved to be from approximately 1-2 years old up to 11 years old.

25. On Tuesday, January 5, 2016, investigators conducted physical surveillance of the SUBJECT PREMISES. They observed two vehicles registered to Nicole Griffin parked at the residence. Investigators performed a wireless network analysis in the area of the SUBJECT PREMISES using a Fluke Aircheck wi-fi tester. The two strongest signals detected were from secured networks, most likely broadcast from the SUBJECT PREMISES. The network analysis identified one weaker, unsecured wireless network in the area, with an SSID of "Aadi-guest."

[5] A NCIC criminal history query yielded negative results for Rhode Island records concerning Ferrante.

26. On January 12, 2016, I spoke by telephone with Theresa Mercado, the Photobucket employee listed as the company contact on Report 6695869. Mercado provided the following information:

(a) Tinypic.com is a photo and video sharing website owned and controlled by Photobucket. Persons using Tinypic.com can post photos or videos on the Tinypic.com website either by creating an account or using the system as a visitor. All photos and videos posted on the Tinypic.com are available for viewing by the public.

(b) Photobucket flags images or videos containing inappropriate or illegal content in two ways: either (i) the image or video contains a word or phrase in the hashtag that suggests inappropriate content or (ii) another Tinypic user reports the inappropriate image or video to Photobucket. Once flagged, the image or video goes into a queue for examination by a Photobucket employee.

(c) Mercado is the employee responsible for examining the flagged files from the Tinypic website. She recalled viewing video file **iqg9z8.flv**.[6] Mercado described observing "a video of a boy giving oral." Mercado initially described the boy as "about 10 years old" but later said that the boy was "probably 7 to 8 years old."

PERSONS WHO POSSESS AND DISTRIBUTE CHILD PORNOGRAPHY

27. As a result of the above-mentioned training and experience, I have learned that the following characteristics are generally found to exist in varying combinations and be true in cases involving offenders who send, cause to be sent, distribute, exhibit, possess, display, transport, manufacture or produce material which depicts minors engaged in sexually explicit conduct. Said material includes, but is not be limited to, photographs, negatives, slides, magazines, other printed media, motion pictures, video tapes, books, or similar items stored electronically on computers, digital devices or related digital storage media.

[6] Mercado could not recall whether video file iqg9z8.flv was flagged for review by Tinypic.com because it contained a word in its hashtag that triggered detection or as a result of another user's report.

28. Individuals who possess, receive, distribute and/or advertise child pornography may receive sexual gratification, stimulation, and satisfaction from (i) contact with children; (ii) from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or (iii) from literature describing such activity;

29. Individuals who possess, receive, distribute and/or advertise child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts;

30. Individuals who possess, receive, distribute and/or advertise child pornography almost always possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years;

31. Likewise, individuals who possess, receive, distribute and/or advertise child pornography often maintain their digital or electronic collections in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained

for several years and are kept close by, usually at the collector's residence, to enable the individual to view the collection, which is valued highly;

32. Individuals who possess, receive, distribute and/or advertise child pornography also (i) may correspond with and/or meet others to share information and materials; (ii) rarely destroy correspondence from other child pornography distributors/collectors; (iii) conceal such correspondence as they do their sexually explicit material; and (iv) often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography; and,

33. Individuals who possess, receive, distribute and/or advertise child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

34. These offenders obtain and/or traffic in materials depicting children engaged in sexually explicit conduct through many sources and by several methods and means. These sources, methods and means include, but are not limited to, the following:

(a) Downloading via the Internet and other computer networks. (Web sites, peer-to peer file sharing networks, newsgroups, electronic bulletin boards, chat rooms, instant message conversations, e-mail, etc.);

(b) Receipt from commercial sources within and outside of the United States through shipments, deliveries and electronic transfer; trading with other persons with similar interests through shipments, deliveries and electronic transfer, including but not limited to email exchanges; and

(c) Producing and manufacturing these materials during actual contact with children or manipulating children into creating such materials and providing them to the perpetrator.

35. Persons who possess and distribute child pornography place significant value on images of child pornography (and related materials). Since child pornography is illegal, it can be risky to obtain. Thus, possessors and distributors of child pornography are very unlikely to destroy or dispose of images once they are obtained. Indeed, it is well-established that possessors and distributors of child pornography hoard their images (and related materials) for many years, rarely, if ever, destroying them. This is particularly true today, when most child pornography is obtained via the Internet and can be easily stored in digital format on a computer or other data storage device. Accordingly, if a possessor or distributor of child pornography saves a digital image on his computer, that image is likely to be present on that computer several years later. Indeed, even if the possessor or distributor of child pornography were to destroy the digital image (or attempt to destroy it), which is rare, it is very likely that the image would still be present on, and recoverable from, the subject's computer years later.

36. In addition to maintaining their images for long periods of time, persons who possess and distribute child pornography almost always maintain and possess their materials within a private location such as their home. In today's computer age, the majority of such images are likely to be maintained in digital form on a computer or other data storage device located in the subject's home. As described above, such images are likely to remain on a subject's computer or other data storage device for many years.

37. Based upon the facts described in Paragraphs 8 through 26 above, there is probable cause to believe that an individual within the SUBJECT PREMISES possessed video file **iqg9z8.flv** on a computer and uploaded that video file to the Internet on September 11, 2015 at 01:59:25 PM (MDT). That individual likely places great value on video file **iqg9z8.flv** and

likely maintains the video – along with other child pornography that s/he has secured – on a computer or other data storage device in the SUBJECT PREMISES to this day.

COMPUTER EVIDENCE

38. Computer hardware, other digital devices, software, and electronic files may be important to a criminal investigation in two distinct ways: (1) the objects themselves may be contraband, evidence, instrumentalities, or fruits of a crime; and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data.

39. In this case, the search warrant application requests permission to search and seize digital media files of child pornography, child erotica and material harmful to minors as well as items indicating illicit contact with minors, including those items that may be stored on a computer, digital device or on electronic media. The images involving sexual conduct of minors constitute both evidence of crime and contraband.

40. This affidavit also requests permission to seize the computer hardware and storage media that may contain the digital media files of child pornography if it becomes necessary for reasons of practicality to remove the hardware and conduct a search off-site. I believe that, in this case, the computer and digital hardware is a container for evidence, a container for contraband and also itself an instrumentality of the crime under investigation.

41. I know from training and experience that computer systems commonly consist of computer processing units (CPU's), hard disks, hard disk drives, floppy disk drives, tape drives, display screens, keyboards, printers, modems (used to communicate with other computers), electronic cables, cassette tapes, floppy disks, and other forms of magnetic and optical media

contain computer information. In addition, the specific transmission of computerized imagery indicates the possible use of CD-ROM / DVD drives, compact laser disks, image scanning devices, still cameras, lighting equipment, video cameras or camcorders, VCRs, digital-analogue translation devices, and the software (computer programming) necessary to operate them.

42. I know from training and experience that such computers and magnetic and optical media are used to store information. In addition to the above mentioned image files, that information often includes data files of other persons engaged in similar activities with minors, and lists of other exploited juveniles, as well as records of correspondence and conversations (printed or electronic) with such persons.

43. I know that information, particularly erased and deleted information, stored within computers and related digital devices can reside within the memory areas of such devices for months and occasionally years. I also know that a qualified computer expert in a laboratory or other controlled environment can recover this information in whole or part.

44. Based on my training and experience, and my discussions with law enforcement electronic forensic examiners, I know that a qualified computer specialist is required to properly retrieve, analyze, document and authenticate electronically stored data, and to prevent the loss of data either from accidental or deliberate programmed destruction. To do this work accurately and completely requires the seizure of (1) all computer equipment and peripherals, which may be interdependent; (2) the software to operate the computer system(s); (3) the instruction manuals, which contain directions concerning the operation of the computer system(s) and software programs; and, (4) all internal and external data storage devices. Each of the seized items should be searched in a laboratory or controlled environment.

45. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a significant amount of time. Indeed, computer specialists, using exacting data search protocols, must often recover hidden, erased, compressed, password-protected, or encrypted files in order to find evidence of criminal activity. Moreover, many commercial computer software programs save data in unique formats that are not conducive to standard data searches. This requires additional effort by specialists to review such data for evidence of a crime. Finally, many users try to conceal criminal evidence by storing files in random order with deceptive file names. This requires specialists to examine all of a user's stored data to determine which particular files are relevant and within the scope of the search warrant. This process can take a substantial amount of time depending on the volume of data stored.

46. Because computer evidence is extremely vulnerable to tampering or destruction, both from external sources or from destructive codes embedded in the system as "booby traps," a controlled environment is essential to a complete and accurate analysis.

47. Data storage devices, including but not limited to hard drives, diskettes and compact disks ("CDs"), can store the equivalent of thousands of pages of information. The majority of computers currently sold have, at a minimum, a 40 gigabyte hard drive, or larger, with an equivalent capacity in excess of 10,000,000 pages of typewritten, double spaced text.

48. For the reasons described in Paragraphs 38 through 48 of this affidavit, it is necessary to seize all computers, data storage devices and related equipment, as described in Attachment B. It is further necessary to search such equipment in a controlled environment, off-

site. Given the potential for large quantities of data, a complete forensic examination of the seized items will take longer than fourteen days.

49. To the extent practical, if persons claiming an interest in the seized computers so request, I will make available to those individuals copies of requested files (so long as those files are not considered contraband) within a reasonable time after the execution of the search warrant. This should minimize any impact the seizures may have on the computer user's personal and/or business operations. In addition, as soon as practical, those items of hardware and software no longer required for the purpose of analysis or copying of items authorized to be seized, or for the preservation of the data and/or magnetic evidence, will be returned to the party from which they were seized, so long as such items do not constitute contraband.

50. Based on my training and experience and my discussions with law enforcement electronic forensic examiners, I know that, in most cases, a trained computer specialist can retrieve deleted image files from a computer or other data storage device, including deleted images of child pornography. Depending on the size of the computer or data storage device, deleted images can be retrieved for years after they have been deleted by the user. Thus, if a user possesses images of child pornography, evidence of those images is likely to be present on his computer or other data storage device years later, regardless of whether the user has deleted or attempted to delete the images

51. In the instant case, there is probable cause to believe that images and/or videos of child pornography are present within the SUBJECT PREMISES on computer(s), devices capable of communicating over the Internet, or other data storage devices and a device that was connected to the Internet service at the SUBJECT PREMISES. Based on my training and

experience, there is probable cause to believe that evidence of those images and/or videos are currently present on a computer, a device capable of communicating over the Internet, or other data storage devices within the SUBJECT PREMISES even if the files have been deleted.

CONCLUSION

52. Based on my training and experience, as well as the information collected by investigators in this investigation, I submit that there is probable cause to believe that contraband and/or evidence, fruits and instrumentalities of the crime of possession of child pornography, in violation of 18 U.S.C § 2252A(a)(5)(B), is presently located at 16 Eustis Street in Worcester, Massachusetts.

53. WHEREFORE, your affiant requests that the Court issue a warrant authorizing investigators to search the SUBJECT PREMISES described in Attachment A for the items described in Attachment B.

BRIAN BISCEGLIA
Task Force Officer
Federal Bureau of Investigations

Subscribed and sworn to before this 13th day of January 2016.

Honorable David H. Hennessy
United States Magistrate Judge

I have reviewed screenshots of video file iqg9z8.flv referenced above and find probable cause to believe that the video depicts a minor engaged in sexually explicit conduct. The U.S. Attorney's Office shall maintain the video for the duration of this case, including any appeals.

Honorable David H. Hennessy
United States Magistrate Judge